

REMARKS

Applicant appreciates the examination of the present application that is evidenced by the Official Action of June 9, 2005. Applicant also appreciates the indication Claims 6-10, 13, 19-20, 24, 29-31, 34-36 and 43 recite allowable subject matter. Claims 48-49 also appear to be in condition for allowance because no rejections or objections of any kind appear to be outstanding with respect to these claims. Applicant has also canceled Claims 1-5, 11-12, 14-15 and 32-33 without prejudice to the filing of a follow-up application. Applicant will now address the outstanding rejections under 35 USC §§ 103 and 112.

The recitation "first time interval" has been properly described in the specification

The specification of the present application provides more than ample description of how the "first time interval" relates to a period of operation of a logic device. For example, at page 2, the specification states: "... *a programmable logic device (PLD) that also generates an encrypted data stream while simultaneously operating under at least partial control of program code during a first time interval.*" (See, e.g., lines 27-29). Thus, by implication, the "first time interval" may have a duration that relates to the length of time that the PLD operates under control of program code. Obviously, this duration will likely vary depending on application and operating environment. Nonetheless, the mere fact that the "time interval" may vary in duration depending on application, does not mean that an insufficient description of this recitation has been provided in the specification.

The specification also describes a relationship between compare operations and the time interval at page 3: "*This circuitry compares the encrypted data streams at least periodically during the first time interval. **** In particular, the encrypted data streams are evaluated at least periodically during the first time interval to determine whether a "match" is present between the authorization device and the proprietary software used to configure the programmable logic device.*" (See, e.g., lines 2-3 and 11-14). Page 4 also provides further support for

when the "time interval" occurs in relationship to device operation: "*These methods preferably include the steps of generating the encrypted data streams during a first time interval while simultaneously operating the programmable logic device under at least partial control of program code that may constitute configuration data.*" (See, e.g., lines 14-19). Here, encrypted data stream generation occurs simultaneously with PLD operation during the time interval.

Page 12 of the specification also provides further support for how the time interval relates to a period of operation:

"The second and third encrypted data streams R and R' are evaluated at least periodically during the first time interval to determine whether a "match" is present between the authorization device 56 and the proprietary "software" loaded into the PLD 54. This evaluation is preferably performed by the authorization detection circuitry ADC 84 within the PLD 54. Thus, a direct ongoing comparison can be made between the encrypted data streams to determine whether there is a sufficiently close identity therebetween, while the PLD 54 is running proprietary software." (See, e.g., lines 9-16).

Based on these highlighted sections from the specification, Applicant respectfully submits that the specification provides ample description to enable one of ordinary skill in the art to understand that a "time interval" relates to a corresponding period of operation of a device when a device is being authorized and the encrypted data streams are being generated and that this period of operation may naturally vary in duration from application to application. Moreover, a starting time point and an ending time point, which specify a duration of the time interval, would also naturally vary depending on when a device begins to operate under authorized control and when the authorized operation of the device is terminated (e.g., device is turned off or encryption operations detect unauthorized operation).

Accordingly, Applicant respectfully requests the Examiner to indicate that Claims 6-10, 13, 19-20, 24, 29-31, 34-36 and 43 are now in condition for allowance along with previously allowed Claims 48-49.

Claims 16-18, 21-23, 25-28, 37-42, 44-47 and 50 Are Patentable
Over the Cited References

Applicant respectfully submits that the cited prior art references to Priem, Thompson and Folmsbee do not disclose the subject matter suggested by the Examiner. In particular, Priem merely discloses an authentication operation that occurs only once prior to commencement of any authorized running of a program and not continuously thereafter using time-varying data streams.

Thompson merely discloses the transmission of descrambling instructions that are received by a descrambling device that also receives video and audio data to be passed downstream to a display (e.g., TV). To add an additional level of security to the received information, the descrambling instructions are also encrypted by the source of the video/audio data. A volatile memory within the receiving device is used to store information need to de-encrypt the incoming instructions from the video/audio information source (e.g., satellite, transmission device). The volatile memory may even store a plurality of descrambling keys so that descrambling operations may be performed on a show-by-show basis. (See, e.g., Thompson, Col. 3, lines 1-46). This volatile memory will lose its de-encryption information if tampered with. However, Thompson, provides absolutely no bidirectional "authorization" communication between the device transmitting the video/audio information (e.g., satellite) and the device receiving the video/audio information (in-home descrambling unit).

Finally, Folmsbee is entirely inapplicable to the claimed invention because the error production operations performed by block 115 (see compiler 41 in FIG. 3) are merely used as a form of "cheap" encryption operations to generate an encrypted data stream. The "errors" within this encrypted data stream are then corrected by an integrated circuit (IC) using a predetermined algorithm.

Accordingly, the inserted errors are not random. This aspect of Folmsbee is described at Col. 7 (lines 1-15):

“Encryption of the software is accomplished, according to one aspect of the present invention, by errors which are intentionally placed in the data and/or into the instructions. The errors are then error-corrected by on-chip circuitry. Since there are a variety of ways to perform error correction, the particular form of error correction is selected at the time of instruction encryption and that particular form of error correction is used to correct the errors on-chip. By way of example, the error correction may be a form of Hamming code. Since there is more than one way to perform this type of error correction, the data or instructions would be essentially useless without providing the information concerning the particular type of Hamming code being used.”

In particular, Folmsbee describes how a “secure key” is used to configure encrypted software within a compiler (see, compiler 41 in FIG. 3). A microprocessor (IC) executing the encrypted software uses non-volatile memory to store an encryption key. This encryption key is used to de-encrypt the encrypted software generated by the compiler – so that the microprocessor can perform the correct operations. (See Folmsbee, Col. 3, lines 43-58).

1. Claims 16-18 Are Patentable Over the Cited References

Claim 16 recites both a programmable logic device (PLD) and an authorization device that are configured to generate respective encrypted data streams. These separate encrypted data streams are compared at least at multiple time points during a first time interval (when the PLD is operating under control of configuration data) to determine whether the PLD is authorized to utilize configuration data during the first time interval.

Contrary to the Examiner’s assertion, a password, such as the password described in Priem, does not automatically represent an “encrypted” stream of

data – even if the password is secret. Of course, a password, like any other data, could undergo an encryption operation, but the mere label “password” does not mean that bits of data that make up the password are by that fact “encrypted”. This same argument applies to the “verification value” described by Priem. Accordingly, Applicant submits that it is improper for the Examiner to treat the password and verification value in Priem as “encrypted data streams.” Moreover, even if Thompson is treated as suggesting the use of a one-way encrypted data stream to prevent unauthorized descrambling of video/audio data, there is no suggestion in Thompson of two separate devices generated separate encrypted data streams that are compared to each other while a PLD, which is operating under control of configuration data, is being checked for authorization to use the configuration data.

Dependent Claim 17 is also independently patentable because it recites how an encrypted data stream is generated in response to a weakly random data stream generated by the PLD during the first time interval. Applicant submits that using a random number generator to generate a key, as described at Col. 11 of Folmsbee, has nothing to do with generating a weakly random data stream and then generating an encrypted data stream from the weakly random data stream.

Finally, with respect to dependent Claim 18, none of the prior art references, even when combined, disclose or suggest generating the second encrypted data stream by evaluating bits in the first encrypted data stream.

2. Claims 21-23 and 25 Are Patentable Over the Cited References

The arguments provided above with respect to Claims 16-18 also apply to Claims 21-23 and 25 and are hereby incorporated herein by reference.

Moreover, with respect to dependent Claim 25, Applicant respectfully submits that Folmsbee's disclosure of the use of a multiplexer at FIG. 2 to select one of many signal lines in response to a control signal has nothing to do with “time division multiplexing” of signals on a bus – which involves sharing of the bus (“time division”) to support bidirectional communication. It is not appropriate for the

Examiner to just pick and chose various elements from various prior art references to reject claims when there is no explicit disclosure or suggestion of the claimed subject matter and no motivation to combine references.

3. Claims 26-28 Are Patentable Over the Cited References

The arguments provided above with respect to Claims 16-18 also apply to Claims 26-28 and are hereby incorporated herein by reference.

4. Claims 37-42 Are Patentable Over the Cited References

The arguments provided above with respect to Claims 16-18, 21-23 and 25 also apply to Claims 37-42 and are hereby incorporated herein by reference. Moreover, dependent Claim 42 recites inserting "random errors" to inhibit reverse-engineering of an encryption operation. Applicant submits that even if Folmsbee can be applied to suggest error generation as a form of encryption, the error generation is not random. Instead, the error generation in Folmsbee (See, FIG. 3, block 115) follows a predetermined algorithm (e.g., Hamming code) that can be reversed by error correction circuit. (See, Folmsbee, Col. 7, lines 1-15).

5. Claims 44-47 and 50 Are Patentable Over the Cited References

The arguments provided above with respect to Claims 16-18, 21-23 and 25 also apply to Claims 44-47 and 50 and are hereby incorporated herein by reference.

In re: Andrew E. Nunns
Serial No. 09/676,748
Filed: September 29, 2000
Page 22

CONCLUSION

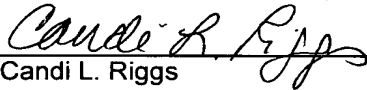
Applicant has shown that the continuous authorization techniques provided by embodiments of the present invention are materially different from the disclosures of the cited prior art references including Priem, Thompson and Folmsbee. Accordingly, Applicant submits that the present application is in condition for allowance, which is respectfully requested. The Examiner is strongly encouraged to contact the undersigned in the event any issues remain which may prevent issuance of the present application.

Respectfully submitted,


Grant J. Scott
Registration No. 36,925

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on October 11, 2005.


Candi L. Riggs

#458290